

ABSTRACT

The present invention protects network devices from overload and from network packet flood attacks (such as Denial of Service and Distributed Denial of Service attacks) that would otherwise consume available resources, and possibly cause system failure or compromise the system by allowing intrusion. The invention, termed an intelligent cache management system is used to free allocated resources (memory, in particular) for reuse, when under sustained attack. One exemplary embodiment of a cache management system of the present invention is used in connection with session-type packet processing devices of a computer network. The system comprises a memory management database for storing communication traffic classification and memory threshold values, and a memory monitor for tracking overall memory usage and determining when the memory threshold values stored in the memory management database are reached. A cache classifier is used to determine a class into which a given session of communications traffic falls. When the memory threshold value is reached, a pruning mechanism selects and prunes entries representing sessions on the packet processing device in accordance with the communication traffic classification and memory thresholds programmed in the memory management database.